DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **24 Jan 13**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Fortinet, Incorporated FortiGate Data Firewalls (DFW) Release (Rel.) 4.3.6

References: (a) Department of Defense (DoD) Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for Interoperability (IO) test certification.

2. The Fortinet DFW Rel. 4.3.6, hereinafter referred to as the System Under Test (SUT), meets all critical IO requirements for joint use within the Defense Information System Network (DISN) as a DFW. The SUT consists of the following Fortinet models: FortiGate DFW 3140B, 620B, 1240B, 5001B, 200B, 3950B, 60C, and 310B. The SUT met all critical IO requirements set forth in Reference (c); using test procedures derived from Reference (d). The SUT operates on the FortiOSv4.3.6 software platform and delivers stable performance by consolidating switching, routing, and security services in a single device. The SUT is certified and approved for joint use within the DISN as a DFW. Although the SUT is a routing device, it was not tested against the Unified Capabilities Requirement (UCR) minimum capabilities and feature requirements for a router and is therefore not certified for joint use as a router. The operational status of the SUT must be verified during deployment. Any new discrepancies that are discovered in the operational environment will be evaluated for impact and adjudicated to the satisfaction of the Defense Information System Agency (DISA) via vendor Plan of Action and Milestones (POA&M) to address the concern(s) within 120 days of identification. No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect IO, but no later than three years from the date of this memorandum.

3. This finding is based on IO testing conducted by JITC, Indian Head, Maryland, from 7 through 11 May 2012. The DISA Certifying Authority (CA) has provided a positive recommendation on 18 December 2012 based on the security testing completed by DISA Information Assurance (IA) test teams and published in a separate report, Reference (e).

4. The Interface, Compatibility Requirements and Functional Requirements, and component status of the SUT are listed in Tables 1 and 2. The threshold Capability/Functional Requirements (CR/FR) for DFWs are established by Section 5.3.8 of Reference (c) and were used to evaluate the IO of the SUT. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

Table 1. SUT Interface Interoperability Status

Interface	Critical	UCR Reference (See note 1.)	Threshold CR/FR (See note 2.)	Status	Remarks (See note 3.)
Data Firewalls					
10Base-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3i (10Base-T) interface were met by these SUT models: All specified SUT models
100Base-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3u (100Base-T) interface were met by these SUT models: All specified SUT models.
1000Base-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3ab (1000Base-T) interface were met by these SUT models: FortiGate 3140B, 620B, 1240B, 5001B, 3950B, 60C, and 310B.
10GBase-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3ae, 802.3AK, 802.3AN, 802.3AQ, and 802.3AV (10000Base-T) interface were met by these SUT models: FortiGate 3140B, 5001B, and 3950B.
40GBase-X	No	5.8	1-4	NA	This interface is not supported and is not required.
100GBase-X	No	5.8	1-4	NA	This interface is not supported and is not required.

NOTES:
1. The UCR 2008, Change 3, Section 5.8 does not identify individual interface requirements for security devices. The SUT provides Ethernet interfaces that meet the requirements in Sections 5.3.2.4 and 5.3.3.10 CR/FR requirements.
2. The CR/FR requirements are contained in Table 2. The CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3, Table 3-1 provides a list of more detailed requirements for DFW products.
3. The specific SUT models listed meet applicable standards for interface provided.

LEGEND:

CR	Capability Requirement	NA	Not Applicable
DFW	Data Firewalls	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements
IEEE	Institute of Electrical and Electronics Engineers		

Table 2. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability (See note.)	UCR Reference	Status	Remarks
Conformance Requirements					
1	Conformance Standards	Required	5.8.4.2	Met	Sub-requirements differ by Security Device type. See Reference (c) for details on data firewalls.
IA Requirements					
2	General Requirements	Required	5.8.4.3.1	Met	Defines IA requirements for Security Devices. Tested by DISA IA test team and results reported separately, Reference (e).
	Configuration Management	Required	5.8.4.3.3	Met	
	Alarms and Alerts	Required	5.8.4.3.4	Met	
	Audit and Logging	Required	5.8.4.3.5	Met	
	Cryptography	Required	5.8.4.3.8	Met	
	Security Measures	Required	5.8.4.3.9	Met	
	System and Communication Protection	Required	5.8.4.3.10	Met	
	Other Requirements	Required	5.8.4.3.11	Met	
	Performance	Required	5.8.4.3.12	Met	
Functionality					
3	Policy	Required	5.8.4.4.1	Met	Sub-requirements differ by Security Device type. These requirements are detailed in Table 3-1.
	Filtering	Required	5.8.4.4.2	Met	
IPv6					
4	IPv6 Requirements	Required	5.3.5	Met	See sub-requirements specified for security devices. See Reference (c) for details on IPv6 requirements.

NOTE: The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3; Table 3-1 provides detailed CR/FR for Data Firewalls.

LEGEND:

CR	Capability Requirements	ID	Identification
DISA	Defense Information Systems Agency	IPv6	Internet Protocol version 6
FR	Functional Requirements	SUT	System Under Test
IA	Information Assurance	UCR	Unified Capabilities Requirement

5. In accordance with the Program Manager's request, JITC did not develop a detailed test report. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Non-secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program, which .mil/.gov users can access on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool at http://jit.fhu.disa.mil (NIPRNet). Information related to Approved Products List (APL) testing is available on the DISA APL Testing and Certification website located at http://www.disa.mil/Services/Network-Services/UCCO. All associated test information is available on the DISA Unified Capability Certification Office APL Integrated Tracking System (APLITS) website located at https://aplits.disa.mil.

6. The JITC point of contact is Mr. Kevin Holmes; commercial (301) 743-4300; e-mail address is Timothy.K.Holmes.civ@mail.mil. The JITC's mailing address is 3341 Strauss Ave., Ste. 236, Indian Head, MD 20640-5035. The tracking number for Fortinet, Inc. FortiGate-3140B Rel. 4.3.6 is 1122002, FortiGate-620B Rel. 4.3.6 is 1122003, FortiGate-1240B Rel. 4.3.6 is 1122004, FortiGate-5001B Rel. 4.3.6 is 1122005, FortiGate-200B Rel. 4.3.6 is 1122006, FortiGate-3950B Rel. 4.3.6 is 1122007, FortiGate-60C Rel. 4.3.6 is 1122009, and FortiGate-310B Rel. 4.3.6 is 1203101.

FOR THE COMMANDER:

Adam K. Britt

3 Enclosures a/s

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
Defense Information Systems Agency, TEMC
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V

ADDITIONAL REFERENCES

(c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 3," September 2011
(d) Joint Interoperability Test Command, "Unified Capabilities Test Plan (UCTP)"
(e) Joint Interoperability Test Command, "Information Assurance (IA) Fortinet FortiGate 3140 Rel. 4 DRAFT IA Assessment Report TN 1122002, Fortinet FortiGate 620B Rel. 4 DRAFT IA Assessment Report TN 1122003, Fortinet FortiGate1240B Rel. 4 DRAFT IA Assessment Report TN 1122004, Fortinet FortiGate5001B Rel. 4 DRAFT IA Assessment Report TN 1122005, Fortinet FortiGate200B Rel. 4 DRAFT IA Assessment Report TN 1122006, Fortinet FortiGate3950 Rel. 4 DRAFT IA Assessment Report TN 1122007, Fortinet FortiGate60C Rel. 4 DRAFT IA Assessment Report TN 1122009, and Fortinet FortiGate FGT_310B Rel. 4.3.6 DRAFT IA Assessment Report TN 1203101"

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Fortinet, Incorporated FortiGate Data Firewalls (DFW) Release 4.3.6.

2. SPONSOR. Mr. Michael Caruso, Marine Corps Network Operations and Security Center Enterprise Services, 27410 Hot Patch Road, Quantico, VA 22134, e-mail: michael.caruso@mcnosc.usmc.mil.

3. SYSTEM POC. Mr. Carl Erickson, 42616 St. Clair Lane, Leesburg, VA 20176, e-mail: cerickson@fortinet.com.

4. TESTER. Joint Interoperability Test Command (JITC), Indian Head, Maryland.

5. SYSTEM DESCRIPTION. Security Devices provide a Global Information Grid (GIG) architectural defense-in-depth capability to protect and define critical warfighting missions. The Unified Capabilities Requirements (UCR) defines three security device products: Data Firewalls and Real Time Services Stateful Firewall; Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS); and Virtual Private Network (VPN) components (concentrator and termination). The DFWs, hereinafter referred to as the System Under Test (SUT) operate on the FortiOS v4.3.6 software platform, which delivers stable performance by consolidating switching, routing, and security services in a single device. The SUT is certified as a DFW only. Although the SUT is a routing device, it was not tested against the UCR minimum capabilities and feature requirements for a router and is, therefore, not certified for joint use as a router. The SUT has a fixed configuration which is ideally suited for securing small distributed enterprise locations.

FortiGate-3140B. Supports Small Form Factor Pluggable (SFP) and Ethernet interfaces that provide up to 58 Gigabit per second (Gbps) firewall throughput, eight 10 Gigabit Ethernet (GbE) SFP+ Local Area Network (LAN) ports, 12 GbE LAN ports, and two 10/100/1000 Megabit per second (Mbps) LAN ports.

FortiGate-620B. Supports Ethernet interfaces that provide 16 Gbps firewall throughput, sixteen 10/100/1000 Mbps accelerated LAN ports, and four 10/100/1000 Mbps standard LAN ports.

FortiGate-1240B. Supports SFP and Ethernet interfaces that provide up to 44 Gbps firewall throughput, 24 SFP ports, 14 GbE LAN ports, and two 10/100/1000 Mbps LAN ports.

FortiGate-5001B. Supports SFP and Ethernet interfaces that provide up to 40 Gbps firewall throughput, eight 10 GbE SFP+ LAN ports, and two 10/100/1000 Mbps LAN

ports. Requires an Advanced Telecom Computing Architecture standard chassis, such as the FortiGate-5060, for operation.

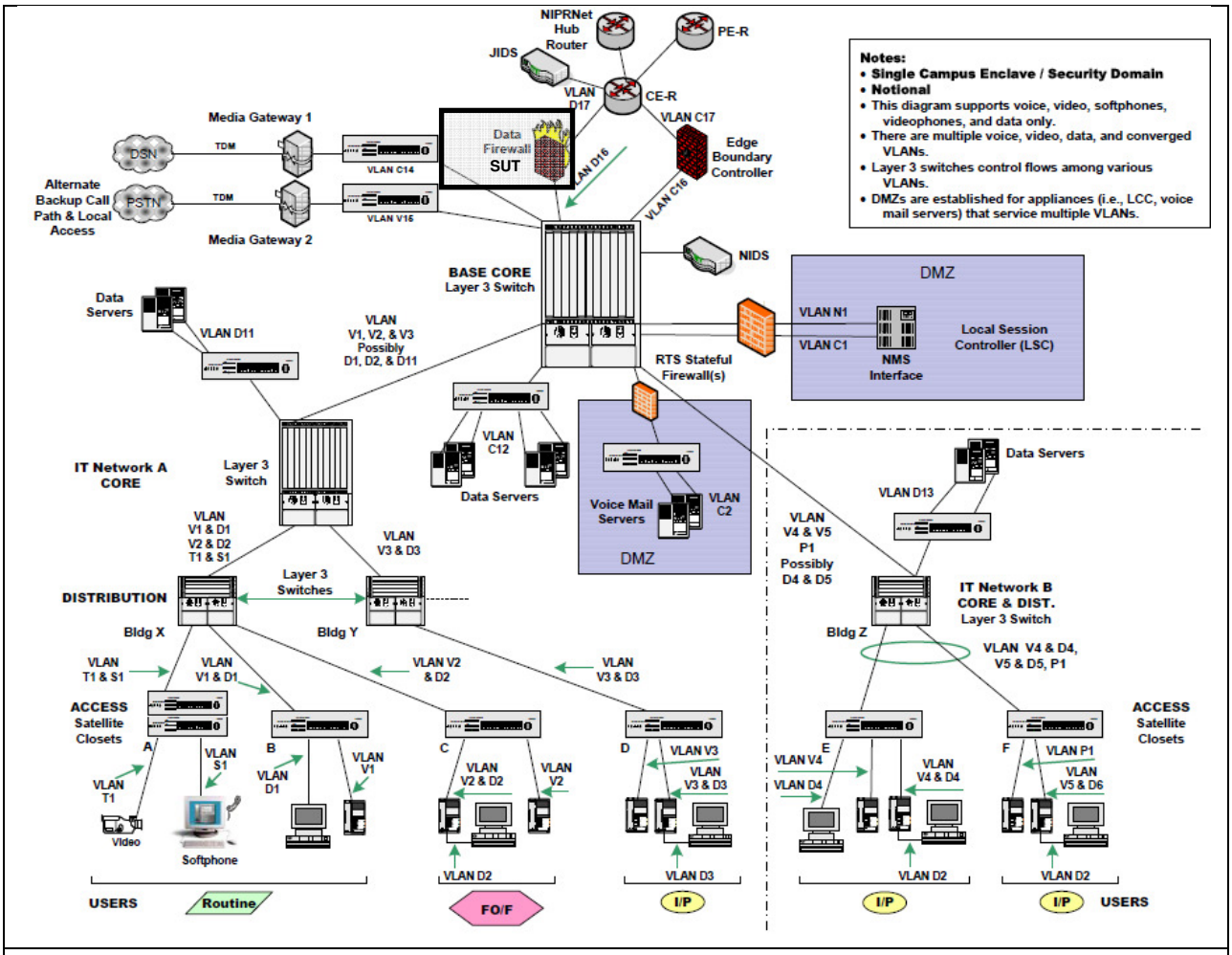
FortiGate-200B. Supports Ethernet interfaces that provide 5 Gbps firewall throughput, eight GbE LAN ports, and eight 10/100 Mbps LAN ports.

FortiGate-3950B. Supports SFP and Ethernet interfaces that provide up to 120 Gbps firewall throughput, two 10 GbE SFP+ LAN ports, 4 GbE LAN ports, and two 10/100/1000 Mbps LAN ports.

FortiGate-60C. Supports Ethernet interfaces that provide one Gbps firewall throughput, two GbE Wide Area Network (WAN) ports, and five GbE LAN ports.

FortiGate-310B. Supports Ethernet interfaces that provide eight Gbps firewall throughput, eight 10/100/1000 Mbps accelerated LAN ports, and two 10/100/1000 Mbps standard LAN ports.

6. OPERATIONAL ARCHITECTURE. Figure 2-1 depicts a notional operational architecture that the SUT may be used in.



LEGEND:

Bldg	Building
CE-R	Customer Edge Router
DIST.	Distribution
DMZ	Demilitarized Zone
DSN	Defense Switched Network
FO/F	Fiber Optics/Fiber
I/P	Input
IT	Information Technology
LCC	Local Call Controller
LSC	Local Session Controller
NIDS	Network Interface Device System
NIPRNet	Non-classified Internet Protocol Network
NMS	Network Management System
PE-R	Provider Edge Router
PSTN	Public Switched Telephone Network
RTS	Real Time Services
SUT	System Under Test
T1	Transmission Link Level 1
TDM	Time Division Multiplexing
VLAN	Virtual Local Area Network

Figure 2-1. Security Device Architecture

7. INTEROPERABILITY REQUIREMENTS. The Interface, Capability Requirements (CR) and Functional Requirements (FR), Information Assurance (IA), and other requirements for security devices are established by Section 5.8 of Reference (c).

7.1 Interfaces. Table 2-1 shows the external interfaces and associated standards that the SUT can use to connect to the GIG network.

Table 2-1. Security Device Interface Requirements

Interface	Critical	UCR Reference (See note 1)	Criteria (See note 2)
10Base-X	No	5.8	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for IEEE 802.3i and 802.3j
100Base-X	No	5.8	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for IEEE 802.3u
1000Base-X	No	5.8	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for IEEE 802.3z
10GBase-X	No	5.8	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for IEEE 802.3ae, 802.3ak, 802.3an, 802.3aq, and 802.3av
40GBase-X	No	5.8	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for IEEE 802.3ba
100GBase-X	No	5.8	Support minimum threshold CRs/FRs 1-4 and meet interface criteria for IEEE 802.3ba

NOTES:
1. The UCR 2008, Change 3, Section 5.8 does not identify individual interface requirements for security devices. The SUT provides Ethernet interfaces that meet Sections 5.3.2.4 and 5.3.3.10 CR/FR requirements.
2. The CR/FR requirements are contained in Table 2-2. The CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for security device products.

LEGEND:

CR	Capability Requirement	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements
IEEE	Institute of Electrical and Electronics Engineers		

7.2 CR and FR. Security Device products have required and conditional features and capabilities that are established by UCR 2008, Change 3, Section 5.8. The SUT does not need to provide non-critical (conditional) requirements. If they are provided, they must function according to the specified requirements. The SUTs features and capabilities and its aggregated requirements in accordance with (IAW) the security device requirements are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of Enclosure 3.

Table 2-2. Security Device CRs and FRs

CR/FR ID	Capability/Function	Applicability (See note.)	UCR Reference	Criteria
1	**Conformance Requirements**			
	Conformance Standards	Required	5.8.4.2	Sub-requirements differ by Security Device type. See Reference (c) for details on data firewalls.
2	**IA Requirements**			
	General Requirements	Required	5.8.4.3.1	Defines IA requirements for Security Devices. These requirements are detailed in Table 3-1.
	Configuration Management	Required	5.8.4.3.3	
	Alarms & Alerts	Required	5.8.4.3.4	
	Audit and Logging	Required	5.8.4.3.5	
	Cryptography	Required	5.8.4.3.8	
	Security Measures	Required	5.8.4.3.9	
	System and Communication Protection	Required	5.8.4.3.10	
	Other Requirements	Required	5.8.4.3.11	
	Performance	Required	5.8.4.3.12	

Table 2-2. Security Device CRs and FRs (continued)

CR/FR ID	Capability/Function	Applicability (See note.)	UCR Reference	Criteria
3	**Functionality**			
	Policy	Required	5.8.4.4.1	Sub-requirements differ by Security Device type. These requirements are detailed in Table 3-1.
	Filtering	Required	5.8.4.4.2	
4	**IPv6**			
	IPv6 Requirements	Required	Table 5.3.5-7	See sub-requirements for specific requirements for security devices. See Reference (c) for details on IPv6 requirements.

NOTE: The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. Table 3-1 provides detailed CR/FR for Data Firewalls.

LEGEND:

CR	Capability Requirements	ID	Identification
FR	Functional Requirements	IPv6	Internet Protocol version 6
IA	Information Assurance	UCR	Unified Capabilities Requirement

7.3 IA. Table 2-3 details the IA requirements applicable to Security Device products.

Table 2-3. Security Device IA Requirements

Requirement	Applicability (See note 1.)	UCR Reference	Criteria
General Requirements	Required	5.8.4.3.1	Meet UCR "required" requirements. Enclosure 3 provides detailed functional requirements for each specified CR/FR
Configuration Management	Required	5.8.4.3.3	
Alarms and Alerts	Required	5.8.4.3.4	
Audit and Logging	Required	5.8.4.3.5	
Cryptography (See note 2)	Required	5.8.4.3.8	
Security Measures	Required	5.8.4.3.9	
System and Communication Protection	Required	5.8.4.3.10	
Other Requirements	Required	5.8.4.3.11	
Performance	Required	5.8.4.3.12	

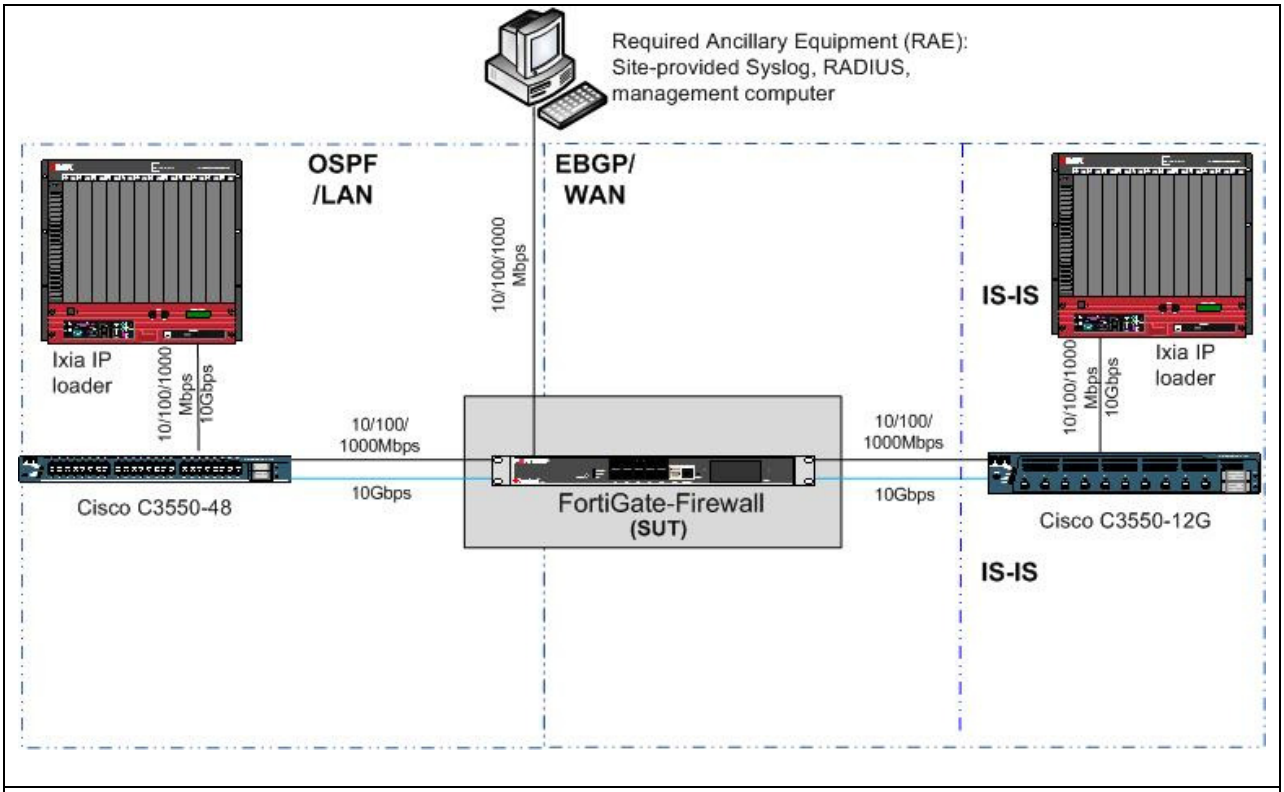
NOTES:
1. Criticality represents high level roll-up of the CR/FR area. Table 3-1 of Enclosure 3 provides detailed CR/FR for each security device product (Data Firewall, IPS, and VPN).
2. Cryptography is optional with the exception that all outgoing communications are encrypted.

LEGEND:

CR	Capability Requirement	IPS	Intrusion Prevention System
FR	Functional Requirement	UCR	Unified capabilities Requirements
IA	Information Assurance	VPN	Virtual Private Network

7.4 Other. None.

8. TEST NETWORK DESCRIPTION. The SUT was tested at the JITC, Indian Head, Maryland, Test Facility in a manner and configuration similar to that of a notional operational environment. Testing the system's required functions and features was conducted using the test configurations depicted in Figure 2-2.



NOTE: Diagram represents the standard testing environment used for each SUT device tested.

LEGEND:

EBGP	Edge Border Gateway Protocol	RADIUS	Remote Authentication Dial In User Service
Gbps	Gigabits per second	RAE	Required Ancillary Equipment
IP	Internet Protocol	SUT	System Under Test
IS-IS	Intermediate System to Intermediate System	SysLog	System Log
LAN	Local Area Network	WAN	Wide Area Network
Mbps	Megabits per second		
OSPF	Open Shortest Path First		

Figure 2-2. SUT Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-4 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic.

Table 2-4. Tested System Configurations

System Name		Equipment
Required Ancillary Equipment		Active Directory
		SysLog
		RADIUS
		Site-Provided management PC
Component	**Release**	**Description**
FortiGate-3140B	FortiOS v4.3.6 (4.0 build 8920 MR3)	FortiGate-3140B Chassis,8 x 10 GbE, 12 x GBE, 2 x 10/100/1000 Mbps no SPC - no NPC
FortiGate-620B		FortiGate-620B Chassis,16 x 10/100/1000 Mbps accelerated, 4 x 10/100/1000 Mbps, no SPC - no NPC
FortiGate-1240B		FortiGate-1240B Chassis, 24 x SFP, 14 x GbE, 2 x 10/100/1000 Mbps no SPC - no NPC
FortiGate-5001B		FortiGate-5001B Chassis, Mid-plane, Power Supply, Fan FortiGate-5001B Module, 8 x 10 GbE, 2 x 10/100/1000 Mbps
FortiGate-200B		FortiGate-200B Chassis, 8 x GbE, 8 x 10/100 Mbps, no SPC - no NPC
FortiGate-3950B		FortiGate-3950B Chassis, 2 x SFP/GbE, 4 x GbE, 2 x 10/100/1000 Mbps no SPC - no NPC
FortiGate-60C		FortiGate-60C Chassis, 2 x GbE WAN, 5 x GbE LAN no SPC - no NPC
FortiGate-310B		FortiGate-310B Chassis, 8 x 10/100/1000 Mbps accelerated, 2 x 10/100/1000 Mbps, no SPC - no NPC
Sub-Component	**Description**	
FortiSwitch 5003B	Switch Module for FortiGate 5001B 10 x SFP/10 GbE	

NOTE: The FortiGate Firewall, as shown is Figure 2-2, is made up of these components

LEGEND:

GbE	Gigabit Ethernet	RADIUS	Remote Authentication Dial In User Service
LAN	Local Area Network	SFP	Small Form Factor Pluggable
Mbps	Megabit per second	SPC	Services Processing Card
MR	Major Release	SysLog	System Log
NPC	Network Processing Card	v	version
OS	Operating System	WAN	Wide Area Network
PC	Personal Computer		

Table 2-5 Non-SUT Equipment

Component	Software Version
Cisco C3550-48	12.2(33)SXJ1
Cisco C3550-12G	12.2(33)SXJ1

LEGEND:
SUT System Under Test

10. TESTING LIMITATIONS. SUT traffic was simulated using network traffic test generation devices. Not every Firewall interface was tested on every SUT model. Each unique interface type was tested, although duplicate interface types on each individual SUT model were not. Each SUT model was evaluated as having the required operation system load, and firewall policy settings.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for DFWs IAW UCR 2008, Change 3, Section 5.8 and is certified for joint use with other network Infrastructure Products listed on the Approved Products List (APL). Additional discussion regarding specific testing results is located in subsequent paragraphs.

11.1 Interfaces. The interface status of the SUT is provided in Table 2-6.

Table 2-6. SUT Interface Requirements Status

Interface	Critical	UCR Reference (See note 1.)	Threshold CR/FR (See note 2.)	Status	Remarks (See note 3.)
Data Firewall					
10Base-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3i (10BaseT) interface where met by these SUT models: All specified SUT models
100Base-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3u (100BaseT) interface where met by these SUT models: All specified SUT models.
1000Base-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3ab (1000BaseT) interface where met by these SUT models: FortiGate 3140B, FortiGate 620B, FortiGate 1240B, FortiGate 5001B, FortiGate 3950B, FortiGate 60C, FortiGate 200B, FortiGate 310B.
10GBase-X	No	5.8	1-4	Met	All critical CRs and FRs for the IEEE 802.3ae, 802.3ak, 802.3an, 802.3aq, and 802.3av (10000BaseT) interface where met by these SUT models: FortiGate 3140B, FortiGate 5001B, FortiGate 3950B.
40GBase-X	No	5.8	1-4	NA	This interface is not supported and is not required.
100GBase-X	No	5.8	1-4	NA	This interface is not supported and is not required.

NOTES:
1. The UCR 2008, Change 3, Section 5.8 does not identify individual interface requirements for security devices. The SUT provides Ethernet interfaces that meet Sections 5.3.2.4 and 5.3.3.10 CR/FR requirements.
2. The CR/FR requirements are contained in Table 2-6. The CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for security device products.
3. The specific SUT models listed meet applicable standards for interface provided.

LEGEND:

CR	Capability Requirement	NA	Not Applicable
FR	Functional Requirement	SUT	System Under Test
IEEE	Institute of Electrical and Electronics Engineers	UCR	Unified Capabilities Requirements

11.2 CR and FR. The SUT CR and FR status is depicted in Table 2-7. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

Table 2-7. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
Conformance Requirements					
1	Conformance Standards	Required	5.8.4.2	Met	Sub-requirements differ by Security Device type. See Reference (c) for details on data firewalls.
IA Requirements					
2	General Requirements	Required	5.8.4.3.1	Met	Defines IA requirements for Security Devices. Tested by DISA IA test team and results reported separately, Reference (e).
	Configuration Management	Required	5.8.4.3.3	Met	
	Alarms & Alerts	Required	5.8.4.3.4	Met	
	Audit and Logging	Required	5.8.4.3.5	Met	
	Cryptography	Required	5.8.4.3.8	Met	
	Security Measures	Required	5.8.4.3.9	Met	
	System and Communication Protection	Required	5.8.4.3.10	Met	
	Other Requirements	Required	5.8.4.3.11	Met	
	Performance	Required	5.8.4.3.12	Met	
Functionality					
3	Policy	Required	5.8.4.4.1	Met	Sub-requirements differ by Security Device type. These requirements are detailed in Table 3-1.
	Filtering	Required	5.8.4.4.2	Met	
IPv6					
4	IPv6 Requirements	Required	5.3.5	Met	See sub-requirements specified for security devices. See Reference (c) for details on IPv6 requirements.

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. Table 3-1 provides detailed CR/FR for Data Firewalls.
2. This is an IA requirement, which was tested by DISA IA test teams and the results published in a separate report, Reference (e).

LEGEND:

CR	Capability Requirements	IPv6	Internet Protocol version 6
DISA	Defense Information Systems Agency	SUT	System Under Test
FR	Functional Requirements	UCR	Unified Capabilities Requirement
IA	Information Assurance		
ID	Identification		

a. Conformance Requirements. Security Devices shall meet the appropriate specific standards described in UCR 2008, Change 3, Section 5.8.4.2, as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

b. IA Requirements.

(1) General Requirements. Security Devices shall meet the appropriate specific standards described in UCR 2008, Change 3, paragraph 5.8.4.3.1, as applicable to DFW products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(2) Configuration Management (CM). Security Devices shall meet the appropriate product specific requirements for CM described in UCR 2008, Change 3,

paragraph 5.8.4.3.3, as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(3) Alarms and Alerts. Security Devices shall meet the appropriate product specific requirements for alarms and alerts described in UCR 2008, Change 3, paragraph 5.8.4.3.4, as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(4) Audit and Logging. Security Devices shall meet the appropriate product specific requirements for audit and logging described in UCR 2008, Change 3, paragraph 5.8.4.3.5 as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(5) Cryptography. Security Devices shall meet the appropriate product specific requirements for cryptography described in UCR 2008, Change 3, paragraph 5.8.4.3.8, as applicable to DFWs, IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(6) Security Measures. Security Devices shall meet the appropriate product specific requirements for security measures as described in UCR 2008, Change 3, paragraph 5.8.4.3.9, as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA-led IA test teams and published in a separate report, Reference (e).

(7) System and Communication Protection. Security Devices shall meet the appropriate product specific requirements for system and communication protection as described in UCR 2008, Change 3, paragraph 5.8.4.3.10, as applicable to Data DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(8) Other requirements. Security Devices shall meet the appropriate product specific requirements for other functional requirements as described in UCR 2008, Change 3, paragraph 5.8.4.3.11, as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(9) Performance. Security Devices shall meet the appropriate product specific requirements for performance as described in UCR 2008, Change 3, paragraph 5.8.4.3.12, as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

c. Functionality.

(1) Policy. Security Devices shall meet the appropriate product specific requirements for policy functionality as described in UCR 2008, Change 3, paragraph 5.8.4.4.1, as applicable to DFWs, IDS/IPS, and VPN products. This was tested by DISA IA test teams and published in a separate report, Reference (e).

(2) Filtering. DFWs shall meet the appropriate product specific requirements for filtering as described in UCR 2008, Change 3, paragraph 5.8.4.4.2. This was tested by DISA IA test teams and published in a separate report, Reference (e).

d. Internet Protocol version 6. The SUT met all critical CRs and FRs with testing and the vendor's Letter of Compliance (LoC).

11.3 IA. Security was tested by DISA IA test teams and published in a separate report, Reference (e).

11.4 Other. None

12. TEST AND ANALYSIS REPORT. IAW the Program Manager's request, no detailed test report was developed. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool at http://jit.fhu.disa.mil (NIPRNet). Information related to APL testing is available on the APL Testing and Certification website at http://www.disa.mil/Services/Network-Services/UCCO.

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The Security Device Products have required and conditional features and capabilities that are established by Section 5.8 of the Unified Capabilities Requirements. The System Under Test need not provide conditional requirements. If they are provided, they must function according to the specified requirements. The detailed Functional Requirements and Capability Requirements for Security Device products are listed in Table 3-1.

Table 3-1. Security Device Products Capability/Functional Requirements Table

ID	Requirement	UCR Ref	FW
1	The security device shall conform to all of the MUST requirements found in RFC 3948, "UDP Encapsulation of IPSec Packets."	5.8.4.2 (15)	R
2	The security device shall support NTPv4.	5.8.4.3.1 (1)	R
3	The security device shall provide ability to push policy to the VPN client and the ability to monitor the client's activity.	5.8.4.3.1 (2)	R
4	The security device shall be managed from a central place, clients, and servers.	5.8.4.3.1 (3)	R
5	The security device shall have five Ethernet ports, one pair for primary ingress and egress, one pair for backup, and one for OOBM.	5.8.4.3.1 (4)	R
6	A CM process shall be implemented for hardware and software updates.	5.8.4.3.3 (1)	R
7	The CM system shall provide an automated means by which only authorized changes are made to the security device implementation.	5.8.4.3.3 (2)	R
8	The security device shall have the ability to disable the Proxy (ARP) service.	5.8.4.3.3 (3)	R
9	The security device shall disable the IP redirects notification service, except in type 3 cases.	5.8.4.3.3 (4)	R
10	The security device shall disable the MOP service in DEC equipment which uses that protocol to perform software loads.	5.8.4.3.3 (5)	O
11	The security device shall disable the source-routing by not forwarding packets with the source-routing IP packet header.	5.8.4.3.3 (6)	R
12	The security device shall properly implement an ordered list policy procedure.	5.8.4.3.3 (7)	R
13	The security device shall apply a set of rules in monitoring events and based on these rules indicate a potential violation of the security device security policy.	5.8.4.3.4 (1)	R
14	The security device shall have the capability to generate an alarm message to a remote administrator console upon detection of a potential security violation.	5.8.4.3.4 (2)	R
15	The security device shall have the capability to generate an alarm message to a new remote administrator's console session if the original alarm has not been acknowledged following a potential security violation.	5.8.4.3.4 (3)	R
16	An automated, continuous online monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential Information Assurance implications.	5.8.4.3.4 (6)	R
17	The security device shall have an automated, continuous online monitoring and audit trail creation capability, which shall be deployed with a user configurable capability to disable the system automatically if serious Information Assurance violations are detected.	5.8.4.3.4 (7)	R
18	The security device shall provide minimum recorded security relevant events including any activity caught by the "deny all" rule at the end of the security device rule base.	5.8.4.3.5 (1)	R

Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref	FW
19	The security device shall generate an audit record of all failures to reassemble fragmented packets.	5.8.4.3.5 (2)	R
20	The security device shall generate an audit record of all attempted uses of the trusted channel functions.	5.8.4.3.5 (3)	R
21	The security device, when configured, shall log the event of dropping packets and the reason for dropping them.	5.8.4.3.5 (4)	R
22	The security device shall log matches to filter rules that deny access when configured to do so.	5.8.4.3.5 (5)	R
23	The security device shall record access or attempted access via security device to all program initiations and shutdowns that have security implications.	5.8.4.3.5 (6)	R
24	The output of such intrusion/attack detection and monitoring tools shall be protected against unauthorized access, modification, or detection.	5.8.4.3.5 (7)	R
25	Security devices that provide encryption services shall be FIPS 140-2, Level 2 compliant.	5.8.4.3.8 (1)	O
26	System mechanisms shall be implemented to enforce automatic expiration of passwords, to prevent password reuse, and to ensure password strength.	5.8.4.3.9 (1)	R
27	Monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns to itself.	5.8.4.3.9 (2)	R
28	The security device's controlled interface shall be configured such that its operational failure or degradation shall not result in any unauthorized release of information outside the IS perimeter nor result in any external information entering the IS perimeter.	5.8.4.3.9 (3)	R
29	Where scanning tools are available, the security device's internal hosts shall be scanned for vulnerabilities in addition to the security device itself to confirm an adequate security policy is being enforced.	5.8.4.3.9 (4)	R
30	The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.	5.8.4.3.9 (5)	R
31	The security device shall drop all packets with an IPv4 non-routable (RFC 1918) address originating from an external source.	5.8.4.3.9 (8)	R
32	The security device shall drop all packets with an IPv4 source address of all zeros.	5.8.4.3.9 (9)	R
33	The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.	5.8.4.3.9 (10)	R
34	The security device shall differentiate between authorized and fraudulent attempts to upgrade the operating system, i.e., trying to upgrade system files with the wrong names.	5.8.4.3.9 (11)	R
35	The security device shall differentiate between authorized and fraudulent attempts to upgrade the configuration, i.e., if a user trying to perform an upgrade that is not authorized that role.	5.8.4.3.9 (12)	R
36	The security device shall pass traffic, which the security device has not identified as being a security problem, without altering the contents, except as necessary to perform functions such as NAT.	5.8.4.3.9 (13)	R
37	The security device shall properly accept or deny UDP traffic from port numbers based on policy.	5.8.4.3.9 (14)	R
38	The security device shall properly accept or deny TCP traffic from port numbers based on policy.	5.8.4.3.9 (15)	R
39	The security device shall not compromise its resources or those of any connected network upon initial start-up of the security device or recovery from an interruption in security device service.	5.8.4.3.9 (16)	R
40	A security device shall properly enforce the TCP state.	5.8.4.3.9 (17)	R
41	A security device shall properly accept and deny traffic based on multiple rules.	5.8.4.3.9 (18)	R
42	A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.	5.8.4.3.9 (19)	R
43	A security device shall prevent the currently available Information Assurance Penetration techniques, as defined in DISA STIGs and IAVAs from penetrating the security device.	5.8.4.3.9 (20)	R
44	A security device shall block potentially malicious fragments.	5.8.4.3.9 (21)	R

Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref	FW
45	The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted.	5.8.4.3.9 (22)	R
46	Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited	5.8.4.3.10 (1)	R
47	The security device's controlled interface shall ensure that only traffic that is explicitly permitted (based on traffic review) is released from the perimeter of the interconnected IS.	5.8.4.3.10 (2)	R
48	The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on a broadcast network.	5.8.4.3.11 (1)	R
49	The security device shall reject requests for access or services where the presumed source identity of the source subject is an external Information Technology entity on the loopback network.	5.8.4.3.11 (2)	R
50	The security device shall permit an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.	5.8.4.3.11 (3)	R
51	The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold: a. Subjects on an internal network can cause information to flow through the security device to another connected network if: (1) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator; (2) The presumed address of the source subject, in the information, translates to an internal network address; (3) And the presumed address of the destination subject, in the information, translates to an address on the other connected network. b. Subjects on the external network can cause information to flow through the TOE to another connected network if: (1) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator; (2) The presumed address of the source subject in the information translates to an external network address; (3) And the presumed address of the destination subject in the information translates to an address on the other connected network.	5.8.4.3.11 (4)	R
52	The security device, after a failure or service discontinuity, shall enter a maintenance mode where the ability to return the security device to a secure state is provided either through manual intervention or automatic reboot.	5.8.4.3.11 (5)	R
53	The security device shall ensure the security policy enforcement functions are invoked and succeed before each function within the security functions scope of control is allowed to proceed.	5.8.4.3.11 (8)	R
54	The security device shall enforce SA Policy regarding Instant Messaging traffic.	5.8.4.3.11 (9)	R
55	The security device shall enforce SA Policy regarding VVoIP traffic.	5.8.4.3.11 (10)	R
56	Access Control shall include a DAC Policy.	5.8.4.3.11 (11)	R
57	DAC access controls shall be capable of including or excluding access to the granularity of a single user.	5.8.4.3.11 (12)	R
58	The security device's controlled interface shall review incoming information for viruses and other malicious code.	5.8.4.3.11 (13)	R
59	The controlled interface shall provide the ability to restore its functionality fully in accordance with documented restoration procedures.	5.8.4.3.11 (14)	R

Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref	FW
60	The developer must specify the security device's bandwidth requirements and capabilities. This shall include the maximum bandwidth speeds the device will operate on, as well as, the security device bandwidth requirements (bandwidth in kbps) documented by who the device communicates with, frequency, and kbps transmitted and received (such as product downloads, signature files).	5.8.4.3.12 (1)	R
61	The security device, as configured, must process new connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (2)	R
62	The security device, as configured, must process new HTTP connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (3)	R
63	The security device, as configured, must process new secure FTP connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	5.8.4.3.12 (4)	R
64	The security device shall employ a commercial best practice defensive solution along with maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack.	5.8.4.3.12 (5)	R
65	The security device must not degrade IPv4 and IPv6 forwarding when used with a long Access Policy configuration.	5.8.4.3.12 (6)	R
66	The security device shall demonstrate a latency variance of less than 20 percent and a packet loss variance of less than 10 percent of the manufacturer specified nominal values for all operational conditions.	5.8.4.3.12 (7)	R
67	The security device shall enforce the policy pertaining to any indication of a potential security violation.	5.8.4.4.1 (1)	R
68	The security device shall be configurable to perform actions based on different information flow policies.	5.8.4.4.1 (2)	R
69	The security device shall deny establishment of an authorized user session based on network source (i.e., source IP address) and time of day parameter values.	5.8.4.4.1 (3)	R
70	The security device shall enforce the system administrator's specified maximum quota of transport-layer open connections that a source subject identifier can use over a specified period.	5.8.4.4.1 (4)	R
71	The security device shall enforce the system administrator's policy options pertaining to network traffic violations to a specific TCP port within a specified period.	5.8.4.4.1 (5)	R
72	The security device shall enforce the system administrator's policy options pertaining to violations of network traffic rules within a specified period.	5.8.4.4.1 (6)	R
73	The security device shall enforce the system administrator's policy options pertaining to any security device-detected replay of data and/or nested security attributes.	5.8.4.4.1 (7)	R
74	This section addresses the ability of a firewall to perform basic filtering functions. It does not mandate a specific filtering configuration for firewalls. The integrity policy adjudication feature known as filtering shall be provided. The security device's controlled interface must support and filter communications protocols/services from outside the perimeter of the interconnected ISs according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications). The security device shall: 1. Have the ability to block on a per-interface basis. 2. Default to block. 3. Default to disabled, if supported on the security device itself. a. Will apply to the following defined services: (1) The service UDP echo (port 7) (2) The service UDP discard (port 9) (3) The service UDP chargen (port 19) (4) The service UDP TCPMUX (port 1) (5) The service UDP daytime (port 13) (6) The service UDP time (port 37) (7) The service UDP supdup (port 95) (8) The service UDP sunrpc (port 111) (9) The service UDP loc-srv (port 135) (10) The service UDP netbios-ns (port 137) (11) The service UDP netbios-dgm (port 138) (12) The service UDP netbios-ssn (port 139) (13) The service UDP BootP (port 67)	5.8.4.4.2	R

Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref	FW
	(14) The service UDP TFTP (port 69) (15) The service UDP XDMCP (port 177) (16) The service UDP syslog (port 514) (17) The service UDP talk (port 517) (18) The service UDP ntalk (port 518) (19) The service UDP MS SQL Server (port 1434) (20) The service UDP MS UPnP SSDP (port 5000) (21) The service UDP NFS (port 2049) (22) The service UDP Back Orifice (port 31337) (23) The service TCP tcpmux (port 1) (24) The service TCP echo (port 7) (25) The service TCP discard (port 9) (26) The service TCP systat (port 11) (27) The service TCP daytime (port 13) (28) The service TCP netstat (port 15) (29) The service TCP chargen (port 19) (30) The service TCP time (port 37) (31) The service TCP whois (port 43) (32) The service TCP supdup (port 95) (33) The service TCP sunrpc (port 111) (34) The service TCP loc-srv (port 135) (35) The service TCP netbios-ns (port 137) (36) The service TCP netbios-dgm (port 138) (37) The service TCP netbios-ssn (port 139) (38) The service TCP netbios-ds (port 445) (39) The service TCP rexec (port 512) (40) The service TCP lpr (port 515) (41) The service TCP uucp (port 540) (42) The service TCP Microsoft UPnP System Services Delivery Point (SSDP) (port 1900) (43) The service TCP X-Window System (ports 6000-6063) (44) The service TCP IRC (port 6667) (45) The service TCP NetBus (ports 12345-12346) (46) The service TCP Back Orifice (port 31337) (47) The service TCP finger (port 79) (48) The service TCP SNMP (port 161) (49) The service UDP SNMP (port 161) (50) The service TCP SNMP trap (port 162) (51) The service UDP SNMP trap (port 162) (52) The service TCP rlogin (port 513) (53) The service UDP who (port 513) (54) The service TCP rsh, rcp, rdist, and rdump (port 514) (55) The service TCP new who (port 550) (56) The service UDP new who (port 550) (57) The service NTP (Network Time Protocol) (58) The service CDP (Cisco Discovery Protocol) (59) Voice and Video Services (AS-SIP), H.323, and RSVP) (60) The service UDP SRTP (SRTCP) and RTCP (61) The service DSCP		
The following requirements are for IPv6			
75	RFC 1981: Path MTU Discovery for IPv6	Table 5.3.5-7	R
76	RFC 2407: The Internet IPSec Domain of Interpretation for ISAKMP	Table 5.3.5-7	C
77	RFC 2408: ISAKMP	Table 5.3.5-7	C
78	RFC 2409: The IKE	Table 5.3.5-7	C
79	RFC 2460: IPv6 Specification	Table 5.3.5-7	R-2
80	RFC 2464: Transmission of IPv6 Packets over Ethernet Networks	Table 5.3.5-7	R-3
81	RFC 2474: Definition of the DS Field in the IPv4 and IPv6 Headers	Table 5.3.5-7	R-4
82	RFC 2710: MLDv2 for IPv6	Table 5.3.5-7	R
83	RFC 3162: RADIUS and IPv6	Table 5.3.5-7	C
84	RFC 3986: URI: Generic Syntax	Table 5.3.5-7	C

Table 3-1. Security Device Products Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref	FW
85	RFC 4007: IPv6 Scoped Address Architecture	Table 5.3.5-7	R
86	RFC 4109: Algorithms for IKEv1	Table 5.3.5-7	C
87	RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers	Table 5.3.5-7	R-1
88	RFC 4291: IPv6 Addressing Architecture	Table 5.3.5-7	R
89	RFC 4301: Security Architecture for the IP	Table 5.3.5-7	C
90	RFC 4302: IP AH	Table 5.3.5-7	C
91	RFC 4303: IP ESP	Table 5.3.5-7	C
92	RFC 4443: ICMPv6 for the IPv6 Specification	Table 5.3.5-7	R
93	RFC 4566: SDP: Session Description Protocol	Table 5.3.5-7	C
94	RFC 4835: Cryptographic Algorithm Implementation Requirements for ESP and AH	Table 5.3.5-7	C
95	RFC 4861: Neighbor Discovery for IPv6	Table 5.3.5-7	R
96	RFC 4862: IPv6 Stateless Address Autoconfiguration	Table 5.3.5-7	C
97	RFC 5095: Deprecation of Type 0 Routing Headers in IPv6	Table 5.3.5-7	R

NOTES:
C/R-1: Only meets the dual-stack requirements of this RFC.
C/R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, WAN General System Requirements.

LEGEND:

AH	Authentication Header
ARP	Address Resolution Protocol
C	Conditional
CM	Configuration Management
DAC	Discretionary Access Control
DISA	Defense Information Systems Agency
DS	Differential Services
DSCP	Differentiated Services Code Point
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FW	Firewall
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAVA	IA Vulnerability Alert
ICMP	Internet Control Message Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS	Information Security
ISAKMP	Internet Security Association and Key Management Protocol
kbps	kilobits per second
MLDv2	Multicast Listener Discovery version 2
MOP	Maintenance Operations Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
OOBM	Out-of-Band Management
R	Required
RADIUS	Remote Authentication Dial-in User Server/Service
Ref	Reference
RFC	Request for Comment
SA	System Administrator
SDP	Session Description Protocol
SRTP	Secure Real-Time Transport Protocol
STIG	Security Technical Implementation Guideline
TCP	Transmission Control Protocol
TSF	Transport Switch Function
UCR	Unified Capabilities Requirement
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VPN	Virtual Private Network
VVoIP	Voice and Video over Internet Protocol
WAN	Wide Area Network